BRUCE L. SIMON (CA SBN 96241)
bsimon@pswlaw.com
ALEXANDER L. SIMON (CA SBN 305734)
asimon@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
44 Montgomery Street, Suite 2450
San Francisco, California 94104
Telephone: (415) 433-9000
Facsimile: (415) 433-9008

DANIEL L. WARSHAW (CA SBN 185365)
dwarshaw@pswlaw.com
MICHAEL H. PEARSON (CA SBN 277857)
mpearson@pswlaw.com
PEARSON SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, California 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

ALEJANDRO SALINAS and MICHAEL RIBONS, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

vs.

EQUIFAX, INC.

Defendant.

CASE NO. 3:17-cv-5284

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1. Alejandro Salinas and Michael Ribons ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this action for damages and injunctive relief against Equifax, Inc. ("Equifax" or "Defendant"). Plaintiffs allege, based on information and investigation of counsel, as follows:

I. NATURE OF THE ACTION

2. On September 7, 2017, Equifax announced the largest and most severe data breach in history; over 143 million people's personal, confidential information had been disclosed to unauthorized third parties between mid-May and July 2017.

3. The information accessed primarily included names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. This information is commonly referred to as personally identifiable information ("PII"). In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with PII for approximately 182,000 U.S. consumers, were accessed.

4. Equifax discovered the data breach on or about July 29, 2017, but did not alert those affected until 40 days later on September 7, 2017 when it issued a press release. In the press release, which was devoid of any substantive information as to how the breach occurred, Chairman and Chief Executive Officer, Richard F. Smith, described the data breach as "a disappointing event."

5. Equifax's conduct – failing to take adequate and reasonable measures to ensure its data systems were protected, failing to prevent and stop the breach from ever happening, failing to disclose to its customers the material facts that it did not have adequate systems and security practices to safeguard customers' financial and personal information, and failing to provide timely notice of the data breach – has exposed the most sensitive PII for over 43% of the United States population.

6. As a result of the Equifax data breach, the personal and confidential information of over 143 million individuals has been exposed to fraud and identity theft and therefore these 143 million customers have been harmed. The injuries suffered by Plaintiffs and the proposed Classes as a direct result of the data breach include:

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

a. Theft of their personal and financial information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their personal information and/or financial accounts;

c. Unauthorized charges on their debit and credit accounts;

d. Loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Equifax data breach;

f. The imminent and certainly impending injury flowing from potential fraud and identify theft posed by their credit card and personal information being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet and/or black market;

g. Damages to and diminution in value of their personal and financial information entrusted to Equifax for the sole purpose of reporting and/or monitoring their credit profile with the mutual understanding that Equifax would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Any money paid for products purchased from Equifax (i.e., credit monitoring, credit score inquiry) at any time before July 29, 2017 when the data breach was discovered as Plaintiffs and Class members would not have engaged Equifax for said services had Equifax disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' financial and personal information; and

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

i. Continued risk to their financial and personal information, which remains in the possession of Equifax and which is subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data.

7. Plaintiffs seek to remedy these harms, and prevent their future occurrence, on behalf of themselves and all similarly situated consumers whose account and/or personally identifying information was stolen as a result of the data breach. Plaintiffs assert claims against Equifax for negligence, violations of state consumer laws, and state data breach statutes. On behalf of themselves and all similarly situated consumers, Plaintiffs seek to recover damages, including actual and statutory damages, and equitable relief, including injunctive relief to prevent a reoccurrence of the data breach, restitution, disgorgement and costs and reasonable attorney fees.

II. PARTIES

A. PLAINTIFFS

8. Alejandro Salinas is a resident of San Francisco County, California whose personal, confidential information, was included in the massive data breach of Defendant's systems and disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

9. Michael Ribons is a resident of Ventura County, California whose personal, confidential information, was included in the massive data breach of Defendant's systems and disclosed to unauthorized third parties and, therefore, was harmed as a direct and proximate result thereof.

B. DEFENDANT

10. Defendant Equifax, Inc. is a Georgia corporation with its headquarters in Atlanta, Georgia. Equifax conducts business throughout the United States, including in this District during the Class Period.

11. Equifax has numerous offices throughout California including in San Rafael, Concord, Palo Alto, Panorama City and Moorpark. Further, its wholly-owned subsidiary and provider of credit monitoring services following the data breach, TrustedID, Inc., is incorporated in Delaware and headquartered in Palo Alto, California.

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

III. JURISDICTION AND VENUE

12. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one Plaintiff and Defendant are citizens of different states. There are more than 100 putative class members.

13. This Court has jurisdiction over Equifax because the company regularly conducts business in California and the other 49 states and has sufficient minimum contacts in California. Equifax intentionally avails itself of this jurisdiction by marketing and selling products to hundreds of millions of consumers nationwide, including in California.

14. This Court has personal jurisdiction Equifax because it: (a) transacted business in the United States, including in this District; (b) directly or indirectly sold or marketed its credit services throughout the United States, including in this District; and/or (c) had substantial aggregate contacts with this District. Defendant conducts business throughout the United States, including in this District, and has purposefully availed itself of the laws of the United States and the State of California.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1931(b)(3) because the Court has personal jurisdiction over Defendant, a substantial portion of the alleged wrongdoing occurred in this District, and Defendant has sufficient contacts with this District.

16. Venue is also proper pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events giving rise to the claims arose in this District, including the actions of TrustedID, Inc., its wholly owned subsidiary, which is located within this District.

IV. FACTUAL ALLEGATIONS

A. EQUIFAX IS ONE OF THREE CREDIT REPORTING GIANTS

17. The Fair Credit Reporting Act, 15 U.S.C. § 1681, ("FCRA") is legislation enacted to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies. It was intended to protect consumers from the willful and/or negligent inclusion of inaccurate information in their credit reports. The FCRA regulates the

collection, dissemination, and use of consumer information, including consumer credit information.

18. Consumer reporting agencies ("CRAs") are entities that collect and disseminate information about consumers to be used for credit evaluation and certain other purposes, including employment. There are three major CRAs—TransUnion, Experian and Equifax.

19. Equifax was founded in Atlanta, Georgia, as Retail Credit Company in 1899. It is currently one of the three major CRAs that collect and disseminate information about consumers to be used for credit evaluation and certain other purposes, including employment. The company organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers.

20. This sensitive financial and personal consumer data is the lifeblood of Equifax's business. Equifax currently operates, or has investments, in 24 countries in North America, Central and South America, Europe and Asia and currently has around 9,900 employees worldwide.

21. Equifax operates in four segments: U.S. Information Solutions ("USIS"), International, Workforce Solutions and Global Consumer Solutions. Its products and services are based on databases of consumer and business information derived from various sources, including credit, financial assets, telecommunications and utility payments, employment, income,

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

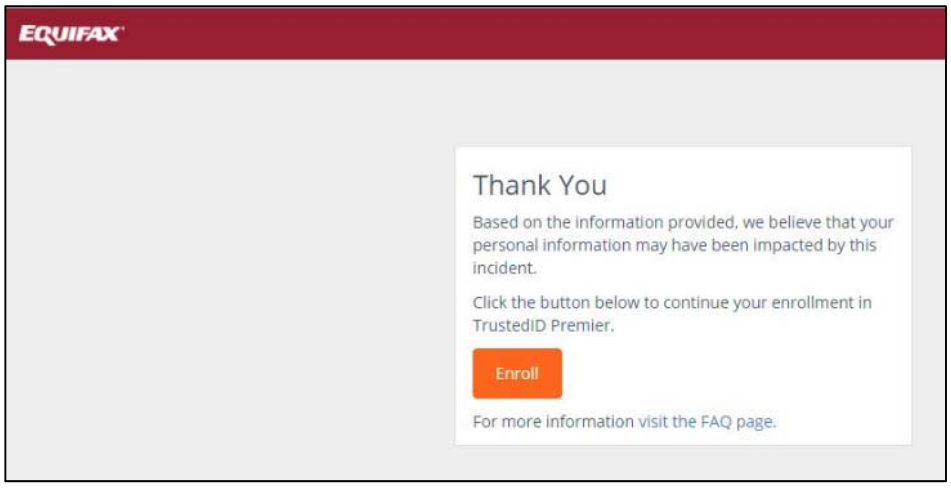
demographic and marketing data. It also helps consumers understand, manage and protect their personal information through credit monitoring services.

22. Equifax has seen wide growth as a company based on its use of sensitive financial and personal consumer data. From 2015 to 2016, the company saw an 18% growth in operating revenues to $3.14 billion and has a current market capitalization of over $14 billion dollars. Richard F. Smith, the Chairman of the Board and Chief Executive Officer of Equifax drew a total compensation package of $14,964,600 in 2016.

B. EQUIFAX ALLOWED THE LARGEST DATA BREACH IN HISTORY

23. On September 7, 2017, Equifax issued a press release announcing that "[c]riminals exploited a U.S. website application vulnerability to gain access to certain files" in Equifax systems. The breach began in mid-May and continued until it was discovered by Equifax on July 29, 2017. The release stated that "[t]he information accessed primarily include[d] names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed. As part of its investigation of this application vulnerability, Equifax also identified unauthorized access to limited personal information for certain UK and Canadian residents." The unauthorized access potentially impacted "approximately 143 million U.S. consumers."

24. Rather than providing piece of mind to customers, upon inputting the requisite information, the following was displayed:



PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

25. Seena Gressin of the Federal Trade Commission ("FTC") commented on the scope of those likely effected by the Equifax data breach; "If you have a credit report, there's a good chance that you're one of the 143 million American consumers whose sensitive personal information was exposed in a data breach at Equifax, one of the nation's three major credit reporting agencies."

26. Experts suggest that as much as 44% of the U.S. population will be affected by the breach, especially with regard to social security numbers which rarely change over a person's lifetime and thus hold resale value on the black market.[1] Even the Social Security Administration itself uses Equifax to help verify the identity of a person when setting up a *my Social Security* account on www.ssa.gov.[2]

27. The Consumer Financial Protection Bureau ("CFPB") has opened an investigation regarding the Equifax data breach and its handling of the same, stating; "The CFPB is authorized to take enforcement action against institutions engaged in unfair, deceptive, or abusive acts or practices, or that otherwise violate federal consumer financial laws. We are looking into the data breach and Equifax's response, but cannot comment further at this time."[3]

28. In light of the potential harm caused, Equifax CEO Richard F. Smith downplayed the largest data security breach in U.S. history by describing it as "a disappointing event" and further stating that he "apologize[s] to consumers and our business customers for the concern and frustration this causes."

C. EQUIFAX KNEW THE RISKS OF A DATA BREACH AND DID NOT TAKE ADEQUATE PRECAUTIONS

29. Equifax knew or should have known that its system was at-risk for attack based on previous attacks and reports that its internal system had weaknesses. Equifax failed to improve its data security after two data breaches that occurred last year: in one, hackers took valuable W-2 tax

---

[1] https://www.wired.com/story/how-to-protect-yourself-from-that-massive-equifax-breach/.
[2] https://www.ssa.gov/.
[3] http://money.cnn.com/2017/09/08/technology/equifax-hack-qa/.

and salary data from the Equifax website and, in another, hackers took W-2 tax data from an Equifax subsidiary called TALX.[4] Cybersecurity professionals interviewed by the New York Times concluded that there should have been more controls in place to prevent the most recent data breach, especially in light of these prior incidents.

30. The first Equifax security breach, which led to a class action lawsuit, stemmed from a May 2016 incident in which Equifax's W-2 Express website was breached, leading to the leak of 430,000 names, addresses, social security numbers, and other information. Equifax had clients' employees access their data with default PIN numbers made up of the last four digits their social security number and four digit year of birth; assigned PIN numbers that were exceedingly easy for criminals to find on the internet. Equifax agreed to fix the underlying issue that led to this data breach, although it is unclear if the vulnerability has yet to be adequately addressed.

31. The second prior Equifax data breach involving TALX was especially alarming because Equifax failed to discover that breach for almost a year—from April 17, 2016 through March 29, 2017. This breach was not publicly disclosed until May 2017. That security breach related to hackers using personal information to guess client customer questions and ultimately reset their 4-digit PIN and gain access to customers' tax data.

32. Equifax also suffered smaller data breaches in January 2017 concerning LifeLock customer credit information, and a 2013-2014 breach of credit reports using personal information. Further, in 2016, a vulnerability to cross-site scripting was discovered. Cross-site scripting, also known as XSS, is a process by which an attacker could send a link they create to users who would click on the link and log on to the website, revealing their user names and passwords and jeopardizing their personal information.

33. Security experts Kenneth White and Kevin Beaumont found that Equifax may have been susceptible to attacks because it uses old and discontinued technology, like Netscape, IBM Websphere, Apache Struts, and Java. The vulnerabilities of those programs should have been

[4] https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#7413fa4f677c

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

addressed sooner given the sensitivity of information and the risk. AlienVault security advocate, Javvad Malik notes that "[c]ompanies like Equifax should know very well that data is the lifeblood of the organization and its crown jewels."

34. Jeff Williams of Contract Security said in an SC Media Magazine article that Apache Struts, which Equifax uses, has two flaws that could have led to the September 2017 data breach: CVE-201-5638, an expression language vulnerability, and CVE-2017-9085, an HTTP request with an unsafe serialized object.[5] These were disclosed in March and September, respectively. Williams believes that the first flaw is a more likely cause because it was publicized in March, giving hackers a chance to exploit it. The fact that this weakness was publicly released in March indicates that Equifax knew or should have known that their system was at risk of breach.

D. EQUIFAX CONCEALED THE BREACH FOR WEEKS WHILE EXECUTIVES CASHED IN

35. Most shockingly, Equifax disclosed that it learned of the unauthorized access on July 29, 2017, but rather than immediately notifying those affected, decided to conceal the information, causing irreparable harm to those whose information was breached. Equifax itself acknowledges the importance of a quick response to a breach of personal and financial data on its own website by stating "[k]nowledge is the best line of defense when it comes to identity theft. The more you know, the better position you'll be in if you're ever a victim."[6]

36. Elsewhere on its website, in a blog post titled "My Identity Has Been Stolen: Now What?" Equifax suggests that anyone whose personal information has been compromised should, among other things, "[s]tart monitoring all your accounts."[7] The post states "[o]f course, the sooner you find out about the problem, the less time has lapsed in which the thief can use your identity" and "[t]he longer the individual's personal information is used unnoticed, the more

---

[5] https://www.scmagazine.com/apache-struts-vulnerability-likely-behind-equifax-breach-congress-launches-probes/article/687955/.

[6] https://www.equifax.com/personal/ (Identity Theft Tab).

[7] https://blog.equifax.com/identity/my-identity-has-been-stolen-now-what/

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

damage is done and the longer it may take to clean up."[8] The post ends by advising customers to "act quickly, take good notes, and stay organized. Make sure to take care of yourself emotionally, as identity theft has many [effects] on victims more far-reaching than the most widely known financial impact."[9]

37. After the most recent Equifax data breach became public, Eric Chaffee, a law professor at University of Toledo and editor of the Securities Law Blog told CNN; "[t]he main problem here is the failure to disclose a catastrophic cyberattack that compromised the information that is at the heart of Equifax's business model." He went on to say that "[t]his created a duty to disclose this attack in a timely fashion to investors, potential investors, and those whose data was compromised." Further, Chaffee found that it was an issue that "[t]he stock price for the last five weeks did not accurately reflect the facts that we now know."

38. Instead of acting quickly to alert the public of the massive breach, Executives executed over $1.8 million in options 48 hours later on August 1, 2017. None of the accompanying regulatory filings lists the transactions as being part of 10b5-1 scheduled trading plans.

39. Regulatory filings show that on August 1, 2017, Chief Financial Officer John Gamble sold 13% of his shares in Equifax worth $946,374 and Joseph Loughran, President of U.S. Information Solutions, exercised options to dispose of 9% of his holdings in Equifax worth $584,099.

40. Regulatory filings also show that on August 2, 2017, Rodolfo Ploder, President of Workforce Solutions, sold $250,458 of stock equivalent to 4% of his holdings in Equifax.

41. Subsequently, on September 8, 2017, the first trading day after the press release regarding the data breach, Equifax (Symbol: EFX) was down 13.66%, a loss of over $2 billion in market cap.

/ / /

---

[8] *Id.*
[9] *Id.*

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

E. THE POST-BREACH MONITORING OFFERED BY EQUIFAX IS INADEQUATE AND DECEIVING

42. After the breach occurred, Equifax told its customers, including Plaintiffs, that it had "established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted" by the breach and to enable them "to sign up for credit file monitoring and identity theft protection."

43. The Equifax breach website says that, in addition to people impacted by the data breach, Equifax is also offering one year of free TrustedID Premier services to anyone in the United States, "[r]egardless of whether your information may have been impacted."

44. By encouraging all consumers to sign up for TrustedID Premier, Equifax stands to profit significantly from the breach of its own computer network.

45. Equifax also benefits when consumers sign up for TrustedID services by gaining access to a wider trove of data.

46. Requiring six digits of your social security number to register for credit monitoring is particularly problematic because a person's entire Social Security Number can be ascertained with just those six digits. To determine the customers' entire Social Security Number an attacker would only have to figure out the first three digits, which is not a difficult task. A Social Security Number consists of nine digits made up of three parts. The first set of three digits is the Area Number, the second set of two digits is the Group Number, and the final set of four digits is the Serial Number.

47. Part one, the Area Number, indicates the geographical region in which the person applied for a social security card. Prior to 1972, states had field offices that issued social security cards and the Area Number assigned represented the state in which the card was issued. However in 1972, the Social Security Administration began issuing cards from a central location in Baltimore for everyone in the nation, so they stopped using the state based Area Numbers. Since 1972, the Area Number assigned is based on the zip code in the mailing address provided on the original application for the Social Security card. Through a little digging or a credit report listing all residences obtained from the Equifax data breach, an immoral actor could piece together the

full social security number and gain easy access to someone else's life past and future. And one cannot get a new Social Security Number.

48. John Ulzheimer—a consumer credit expert—noted in a New York Times article that one year of the free protection service from Equifax does not completely protect consumers because their information can still be sold for several years after the one year of protection is over.

49. Rich Mogull who operates a security research firm called Securosis went a step further in an ABC News article, saying, "[i]f any of the data was exposed, you will be living with that for the rest of your life."

F. PLAINTIFFS AND HUNDREDS OF MILLIONS OF OTHERS WERE INJURED

50. The FTC website suggests that people consider freezing their credit reports in light of the Equifax incident, but this can be inconvenient in that it keeps consumers from opening new accounts unless they unfreeze them days in advance.

51. Further, even if consumers freeze their credit reports with Equifax, they must also freeze them for both Experian and TransUnion as well to give them the best protection.

52. To add cost to this inconvenience of freezing credit reports, in some states these companies require consumers to pay a fee to freeze and unfreeze their credit reports.

53. Unfortunately, even if consumers freeze their credit reports, they are not protected from fraudulent tax returns being filed with their information or people using their credit cards.

54. Security analyst at Gartner, Avivah Litan is quoted in a USA Today article as saying that instead of checking credit card statements monthly, people need to now check them weekly and be hyper-vigilant if their information has been jeopardized. This is a further inconvenience that those affected by the Equifax data breach, including Plaintiffs, must endure.

55. In addition to common fears relating to identity theft like credit card use, people opening accounts in another person's name, and harm to a credit score, consequences like medical identity theft (fake IDs used to pay for procedures and surgeries), tax fraud (filing false tax returns to profit from refunds), and synthetic identity theft (combining information from multiple victims to create a new identity) are also possible because of the depth of information stolen.

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

56. On Friday, September 8, 2017, New York Attorney General Eric Schneiderman issued a press release indicating that he has launched an investigation into the Equifax data breach and sent a letter to Equifax seeking additional information about the breach. "The Equifax breach has potentially exposed sensitive personal information of nearly everyone with a credit report, and my office intends to get to the bottom of how and why this massive hack occurred," said Schneiderman.

57. Following the Equifax press release, the CFPB's Senior Spokesperson Sam Gilford said the Bureau is looking into the situation. Further, Gilford stated that: "The CFPB has authority over the consumer reporting industry, including supervisory and enforcement authority," and that "[t]he CFPB is authorized to take enforcement action against institutions engaged in unfair, deceptive, or abusive acts or practices, or that otherwise violate federal consumer financial laws[.]"

58. The House Financial Services Committee is also launching an investigation into the breach.

V. CLASS ALLEGATIONS

59. Plaintiffs bring this action both on behalf of themselves and all others similarly situated (the "Classes") pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2) and (b)(3). The Classes are defined as follows:

60. A "Nationwide Negligence Class" seeking damages, equitable and injunctive relief defined as follows:

> All persons and entities in the United States whose personal, confidential information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017. Excluded from the Class are Defendant; Defendant's affiliates, subsidiaries or co-conspirators; employees of Defendant, including its officers and directors; and the Court to which this case is assigned.

/ / /

/ / /

/ / /

/ / /

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

61. The "California Class" seeking damages, equitable and injunctive relief defined as follows:

> All residents of the State of California whose personal, confidential information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017. Excluded from the Class are Defendant; Defendant's affiliates, subsidiaries or co-conspirators; employees of Defendant, including its officers and directors; and the Court to which this case is assigned.

62. Following further investigation as well as discovery in the case, definitions of the Classes, including the Class Periods defined above, may be modified by amendment, and Plaintiffs reserve the right to join additional class representatives.

63. *Numerosity*. The Classes are individually so numerous that joinder of all members is impracticable. Even though the exact number of members of the Class is unknown at this time, Equifax has represented that at least 143 million individuals are affected by the data breach and that their identities can be readily ascertained from records in the possession of Defendant.

64. Class members are geographically dispersed throughout the United States and its territories.

65. *Ascertainability*. All members of the purposed Classes are readily ascertainable. Equifax has access to addresses and other contact information for millions of members of the Classes, which can be used for providing notice to many Class members.

66. *Typicality*. Plaintiffs' claims are typical of the claims of the other members of the Classes because the same events and conduct that give rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member. Plaintiffs and the Class members were similarly affected by the Defendants' uniform wrongful and unauthorized disclosure of personal, confidential information to unauthorized third parties.

67. *Adequacy*. Plaintiffs will fairly and adequately protect the interests of the Classes and have retained counsel competent and experienced in class action, antitrust and consumer protection litigation. Plaintiffs' interests are coincident with, and not antagonistic to, the interests of the Classes.

/ / /

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

68. *Commonality.* Common questions of law and fact exist as to all members of the Classes and predominate over any questions solely affecting individual Class members.

69. Plaintiffs and members of the Classes have all sustained damages during the Class Period as a result of having their personal, confidential information disclosed to unauthorized third parties by Defendant. Defendant's conduct alleged herein, the impact of such conduct, and the relief sought are all issues or questions that are common to Plaintiffs and the Classes.

70. The questions of law and fact common to the Classes include, but are not limited to:

i. Whether Equifax engaged in the wrongful conduct alleged herein;

ii. Whether Equifax owed a duty to Plaintiffs and members of the Classes to adequately protect their personal, confidential information and to provide timely and accurate notice of the data breach to Plaintiffs and members of the Classes;

iii. Whether Equifax breached its duty to protect the personal, confidential information of Plaintiffs and members of the Classes by failing to provide adequate data security;

iv. Whether Equifax breached its duty to provide timely and accurate notice to Plaintiffs and members of the Classes of the data breach;

v. Whether Equifax knew or should have known that its systems were vulnerable to attack;

vi. Whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of millions of consumers' personal, confidential data;

vii. Whether Equifax unlawfully failed to inform Plaintiffs and members of the Classes that it did not maintain computers and security practices adequate to reasonably safeguard customers' personal, confidential data and whether Equifax failed to inform Plaintiffs and members of the Classes of the data breach in a timely and accurate manner;

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

viii. Whether Plaintiffs and members of the Classes were injured by Defendant's conduct (or failure to act), and, if so, the appropriate class-wide measure of damages for Class members;

ix. Whether Plaintiffs and members and Classes are entitled to recover damages; and

x. Whether Plaintiffs and Class members are entitled to equitable relief, including injunctive relief and/or other equitable relief.

71. *Superiority.* A class action is superior to other available methods for the fair and efficient adjudication of this controversy because joinder of all members of the Classes is impracticable.

72. The prosecution of separate actions by individual members of the Classes would impose heavy burdens upon the courts and the parties, and would create a risk of inconsistent or varying adjudications of the questions of law and fact common to the Classes. A class action would achieve substantial economies of time, effort, and expense, and would assure uniformity of decision as to persons similarly situated without sacrificing procedural fairness. There will be no material difficulty in the management of this action as a class action on behalf of the Class. Although the laws of different states are implicated in this Complaint, these laws are substantially similar to one another and can be grouped together in manageable categories.

73. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(3). The above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

74. Certification of the Class is also appropriate pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), and/or (c)(4).

/ / /

/ / /

/ / /

/ / /

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

VI. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Negligence
(Nationwide Negligence Class)

75. Plaintiffs incorporate and reallege, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

76. Equifax owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their personal and financial information in its possession from being compromised, lost stolen, accessed, and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Equifax's security system to ensure that Plaintiffs' and the Class's personal and financial information in Equifax's possession was adequately secured and protected. Equifax further owed a duty to Plaintiffs and the Class to implement processes that would detect a breach of it security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

77. Equifax owed a duty to Plaintiffs and the Class to provide security, including consistent with industry standards and requirements, to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the personal and financial information of Plaintiffs and the Class whose personal and financial information was obtained by Equifax.

78. Equifax owed a duty of care to Plaintiffs and the Class because they were foreseeable and probable victims of any inadequate security practices. Equifax solicited, gathered, and stored the personal and financial data of Plaintiffs and the Class to facilitate credit reports and monitoring. Equifax knew it inadequately safeguarded such information on its computer systems and that hackers routinely attempt to access this valuable data without authorization. Equifax had prior notice that its systems were inadequate by virtue of the earlier breaches that preceded this one, but continued to maintain those inadequate systems to the ultimate detriment of its customers like Plaintiffs. Equifax knew or should have known that a breach of its systems would cause

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

damages to Plaintiffs and the Class and Equifax had a duty to adequately protect such sensitive personal and financial information.

79. Equifax owed a duty to timely and accurately disclose to Plaintiffs and the Class that their personal and financial information had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate, and necessary so that, among other things, Plaintiffs and the Class could take appropriate measures to avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Equifax's misconduct.

80. Equifax knew, or should have known, the risks inherent in collecting and storing the personal and financial information of Plaintiffs and the Class, and of the critical importance of providing adequate security of that information.

81. Equifax's own conduct also create a foreseeable risk of harm to Plaintiffs and the Class. Equifax's misconduct included, but was not limited to, its failure to take steps and opportunities to prevent and stop the data breach as set forth herein.

82. Equifax breached the duties it owed to Plaintiffs and the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the personal and financial information of Plaintiffs and the Class.

83. Equifax breached the duties it owed to Plaintiffs and the Class by failing to properly implement technical systems or security practices that could have prevented the loss of data at issue.

84. Equifax breached its duties to timely and accurately disclose that Plaintiffs' and the Class's personal and financial information in Equifax's possession had been or was reasonably believed to have been stolen or compromised.

85. Equifax's failure to comply with its legal obligations under California Civil Code §§ 1798.80, *et seq*. by causing delay between the date of intrusion and the date Equifax disclosed

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

the data breach further evidence Equifax's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class's personal and financial information in Equifax's possession.

86. But for Equifax's wrongful and negligent breach of its duties owed to Plaintiffs and the Class, their personal and financial information would not have been compromised.

87. The injury and harm suffered by Plaintiffs and the Class, as set forth above was the reasonably foreseeable result of Equifax's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class's personal and financial information within Equifax's possession. Equifax knew or should have known that its systems and technologies for processing, securing, safeguarding, and deleting Plaintiffs' and the Class's personal and financial information were inadequate and vulnerable to being breached by hackers.

88. Plaintiffs and the Class suffered injuries and losses described herein as a direct and proximate result of Equifax's conduct resulting in the data breach, including Equifax's lack of adequate reasonable and industry-standard security measures. Had Equifax implemented such adequate and reasonable security measures, Plaintiffs and the Class would not have suffered the injuries alleged, as the Equifax data breach would likely have not occurred.

89. A special relationship exists between Plaintiffs and the Class and Equifax.

90. Equifax collects personal and financial data from Plaintiffs and the Class to create credit scores and monitor credit activity, including during the period of the Equifax data breach. Plaintiffs and the Class allowed this to happen with the mutual understanding that Equifax had reasonable security measures in place to protect its customers' personal and financial information.

91. Equifax's conduct warrants moral blame, as Equifax continued to take possession of Plaintiffs' and the Class's personal and financial information in connection with its Services knowing, and without disclosing, that it had inadequate systems to reasonably protect such information and even after the data breach had occurred and was ongoing, and Equifax failed to provide timely and adequate notice to Plaintiffs and the Class as required by law.

92. Holding Equifax accountable for its negligence will further the policies underlying negligence law and will require Equifax and encourage similar companies that obtain and retain

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

sensitive consumer personal and financial information to adopt, maintain and properly implement reasonable, adequate and industry-standard security measures to protect such customer information.

93. Equifax's special relationship with Plaintiffs and the Class further arises from Equifax's special and critically important obligations under California Civil Code §§ 1798.81.5 and 1798.82. Section 1798.81.5 requires Equifax to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information" and Section 1798.82 requires Equifax to give notice to Plaintiffs and the Class in case of a breach "in the most expedient time possible and without unreasonable delay." Equifax failed to fulfill its obligations to Plaintiffs and the Class arising under California Civil Code §§ 1798.81.5 and 1798.82 in that Equifax failed to maintain and properly implement reasonable, adequate and industry-standard security measures to protect personal and financial customer information and to give expedient notice to Plaintiffs and the Class of the breach.

94. As a direct and proximate result of Equifax's negligent conduct, Plaintiffs and the Class have suffered injury and are entitled to damages in the amount to be proven at trial.

SECOND CLAIM FOR RELIEF
Violation of California Customer Records Act
(Cal. Civil Code §§ 1798.80, *et seq*.)
(California Class)

95. Plaintiffs incorporate and reallege, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

96. California Civil Code § 1798.81.5 clearly and expressly states the intent of the legislature: "It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information."

97. Further, California Civil Code § 1798.81.5(b) requires any "business that owns, licenses, or maintains personal information about a California resident [to] implement and maintain reasonable security procedures and practices appropriate to the nature of the information,

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

98. Equifax owns, maintains, and licenses personal information, within the meaning of § 1798.81.5, concerning Plaintiffs and the California Class.

99. Equifax violated Civil Code § 1798.81.5 by failing to implement reasonable measures to protect the personal information of the members of the California Class.

100. The data breach described above occurred as a direct and proximate result of Equifax's violations of section 1798.81.5 of the California Civil Code.

101. California Civil Code § 1798.82(a) provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay… ."

102. California Civil Code § 1798.2(b) provides that "[a] person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

103. Equifax is a business that owns or licenses computerized data that includes personal information as defined by California Civil Code §§ 1798.80, *et seq*.

104. In the alternative, Equifax maintains computerized data that includes personal information that it does not own as defined by California Civil Code §§ 1798.80, *et seq*.

105. The personal information (including but not limited to names, birth dates, and Social Security numbers) of the members of the California Class includes personal information covered by California Civil Code § 1798.81.5(d)(1).

/ / /

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

106. Because Equifax reasonably believed that the personal information of the members of the Class was acquired by unauthorized persons, it had an obligation to disclose the data breach described above in a timely and accurate fashion under California Civil Code § 1798.82(a), or in the alternative, under California Civil Code § 1798.82(b).

107. Thus, by failing to disclose the data breach in a timely and accurate manner, Equifax violated California Civil Code § 1798.82.

THIRD CLAIM FOR RELIEF
Violation of Unfair Competition Law
(Cal. Bus. & Prof. Code §§ 17200, *et seq*.)
(California Class)

108. Plaintiffs incorporate and reallege, as though fully set forth herein, each and every allegation set forth in the preceding paragraphs of this Complaint.

109. Defendant has engaged in unfair competition within the meaning of California Business & Professions Code §§ 17200, *et seq*. (the "UCL") because Defendant's conduct is unfair and unlawful as herein alleged. Plaintiffs and members of the California Class were injured by Defendant's conduct because Equifax failed to properly maintain Plaintiffs' and the California Class's personal and financial information and unreasonably delayed in informing the public, including Plaintiff and the California Class, about the breach of security of Plaintiffs' and the California Class's confidential and nonpublic personal information after Equifax knew or should have known that the data breach had occurred.

110. Defendant's business practices, and each of them, are unfair because they offend established public policy and/or are immoral, unethical, oppressive, unscrupulous and/or substantially injurious to consumers in that Plaintiffs and the California Class suffered harm directly resulting from Equifax's failure to properly maintain Plaintiffs' and the California Class's personal and financial information and failed to provide Plaintiffs and the California Class with timely and accurate notice. Plaintiffs and the California Class suffered the damages alleged above as a direct result of Equifax's failure to properly maintain Plaintiffs' and the California Class's personal and financial information and delay in providing timely and accurate notice of the data breach. This failure constitutes a violation of the UCL.

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

111. The Class is further injured when Defendant continued to operate without having proper security protocols in place. Equifax failed to exercise reasonable care in implementing and maintaining reasonable procedures and practices appropriate for maintaining the safety and security of Plaintiffs' and the Class's personal and financial information in its possession, custody, and/or control. This failure constitutes a violation of the UCL.

112. Defendant's business practices are unlawful and violates California Civil Code §§ 1798.81.5 and 1798.82 as more fully set forth above.

113. Plaintiffs and the California Class are entitled to relief, to the greatest extent permitted by law, which may not have been obtained by Defendant as a result of such business acts or practices, and enjoining Defendant from engaging in the practices described herein in the future.

114. Plaintiffs are entitled to an award of attorneys' fees and costs pursuant to, *inter alia*, California Code of Civil Procedure § 1021.5.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that the Court:

A. Determine that the claims alleged herein may be maintained as a Class action under Rule 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, and Order that reasonable notice of this action be given to members of the Classes;

B. Appoint Plaintiffs as Class Representatives for the Classes, and Counsel of Record as Lead Class counsel;

C. That the Court award Plaintiffs and the Classes appropriate relief to the maximum extent allowed, and enter a joint and several judgment in favor of Plaintiffs and the members of such classes against Defendant, including actual and statutory damages;

D. That the Court award Plaintiffs and the Classes equitable, injunctive and declaratory relief as maybe appropriate under applicable state laws. Plaintiffs, on behalf of the Classes, seek appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing the best security data practices to safeguard customers' financial and personal information and that would include, without limitation, an order and

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

judgment directing Equifax to (1) encrypt and protect all data and (2) directing Equifax to provide to Plaintiffs and Class members extended credit monitoring services.

E. Award Plaintiffs and the members of the Classes pre- and post- judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of this Complaint;

F. Award Plaintiffs and the members of the Classes their costs of suit, including reasonable attorneys' fees, as provided by law; and,

G. Award Plaintiffs and members of the Classes such other and further relief as the case may require and the Court may deem just and proper.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104

VIII. DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury, including pursuant to Federal Rule of Civil Procedure 38(b), on all issues where a right to such trial exists.

DATED: September 12, 2017

PEARSON, SIMON & WARSHAW, LLP

SCHNEIDER WALLACE COTTRELL KONECKY WOTKYNS LLP

By: */s/ Daniel L. Warshaw*
DANIEL L. WARSHAW

DANIEL L. WARSHAW (CA SBN 185365)
dwarshaw@pswlaw.com
MICHAEL H. PEARSON (CA SBN 277857)
mpearson@pswlaw.com
PEARSON SIMON & WARSHAW, LLP
15165 Ventura Boulevard, Suite 400
Sherman Oaks, California 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104

BRUCE L. SIMON (CA SBN 96241)
bsimon@pswlaw.com
ALEXANDER L. SIMON (CA SBN 305734)
asimon@pswlaw.com
PEARSON, SIMON & WARSHAW, LLP
44 Montgomery Street, Suite 2450
San Francisco, California 94104
Telephone: (415) 433-9000
Facsimile: (415) 433-9008

TODD M. SCHNEIDER (CA SBN 158253)
tschneider@schneiderwallace.com
KYLE G. BATES (CA SBN 299114)
kbates@schneiderwallace.com
SCHNEIDER WALLACE COTTRELL KONECKY WOTKYNS LLP
2000 Powell Street, Suite 1400
Emeryville, California 94608
Telephone: (415) 421-7100
Facsimile: (415) 421-7105

Attorneys for Plaintiffs Alejandro Salinas and Michael Ribons

PEARSON, SIMON & WARSHAW, LLP
44 MONTGOMERY STREET, SUITE 2450
SAN FRANCISCO, CALIFORNIA 94104